แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ

(IT Contingency Plan)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงยุติธรรม

---

๑. หลักการและเหตุผล

สำนักงานปลัดกระทรวงยุติธรรมได้พัฒนาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อช่วยเพิ่มศักยภาพการดำเนินงานในการให้บริการประชาชนและหน่วยงานต่างๆ ระบบเทคโนโลยีสารสนเทศอาจมีความเสี่ยงที่จะได้รับความเสียหาย ไม่สามารถใช้งานได้อย่างต่อเนื่อง จากการถูกโจมตี จากไวรัสคอมพิวเตอร์ บุคลากร ภัยธรรมชาติ หรือปัจจัยทั้งภายในและภายนอกต่างๆ ซึ่งส่งผลกระทบต่อการดำเนินงานของสำนักงานปลัดกระทรวงยุติธรรม

เพื่อป้องกันและแก้ไขปัญหาดังกล่าว สำนักงานปลัดกระทรวงยุติธรรม โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเห็นความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศทำให้ระบบเทคโนโลยีสารสนเทศสามารถใช้งานได้อย่างต่อเนื่อง และมีประสิทธิภาพ

๒. วัตถุประสงค์

๒.๑ เพื่อเป็นแนวทางในการควบคุมและบำรุงรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้มีความเสถียร มีความพร้อมสำหรับการใช้งาน

๒.๒ เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้ทันท่วงที

๒.๔ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ สร้างความเข้าใจและตระหนักในการบำรุงรักษาระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงยุติธรรม

๓. การประเมินสถานการณ์ความเสี่ยง

จากการศึกษาวิเคราะห์ระบบเทคโนโลยีสารสนเทศ ของสำนักงานปลัดกระทรวงยุติธรรม พบว่าความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ มีดังนี้

๓.๑ เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error)

เจ้าหน้าที่หรือบุคลากรของหน่วยงานอาจรู้เท่าไม่ถึงการณ์ หรือขาดความรู้ความเข้าใจการใช้งานที่ถูกต้อง อันอาจทำให้ระบบเทคโนโลยีสารสนเทศได้รับความเสียหาย จนไม่สามารถใช้งานได้หรือหยุดการทำงาน ซึ่งจะส่งผลให้ไม่สามารถใช้งานได้หรือใช้งานได้ไม่เต็มประสิทธิภาพ

๓.๒ เกิดจากไวรัสคอมพิวเตอร์ หรือการถูกเจาะระบบ

มีโอกาสเกิดความเสี่ยงจากการถูกผู้ไม่ประสงค์ดี ได้แก่ Hacker หรือไวรัสคอมพิวเตอร์บุกรุกหรือทำลายระบบคอมพิวเตอร์และเครือข่ายทำให้เกิดการหยุดชะงัก หรือใช้งานไม่ได้ หรือขโมยข้อมูลสำคัญขององค์กรไป

๓.๓ เกิดจากระบบไฟฟ้าขัดข้อง

มีโอกาสเกิดความเสี่ยงจากการเกิดกระแสไฟฟ้าตก ไฟฟ้าดับ ฟ้าผ่าทำให้เกิดไฟฟ้ากระชากกระแสไฟฟ้าเกิน ซึ่งทำให้ระบบเครื่องคอมพิวเตอร์ได้รับความเสียหาย และระบบเครือข่ายหยุดชะงักไม่สามารถให้บริการได้

๓.๔ เกิดจากโจรกรรม

มีโอกาสเกิดความความเสียหายจากการโจรกรรมอุปกรณ์คอมพิวเตอร์และเครือข่าย ซึ่งมีผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร อาจถึงขั้นทำให้ระบบเทคโนโลยีสารสนเทศหยุดชะงัก ไม่สามารถให้บริการต่อไปได้

๓.๕ เกิดความเสียหายจากเพลิงไหม้

มีโอกาสเกิดความเสียหายที่จะเกิดเพลิงไหม้จากความรู้เท่าไม่ถึงการณ์ ความประมาท หรือจากอุบัติเหตุได้ เช่น ไฟฟ้าลัดวงจร เป็นต้น อาจนำมาซึ่งความสูญเสียอย่างใหญ่หลวงกับระบบเทคโนโลยีสารสนเทศทำให้หยุดชะงัก ไม่สามารถให้บริการได้

๓.๖ เกิดความเสียหายจากการเกิดอุบัติภัยทางธรรมชาติ

มีโอกาสเกิดความเสียหายจากอุบัติภัยทางธรรมชาติที่มีผลกระทบต่อการให้บริการระบบเทคโนโลยีสารสนเทศและการสื่อสาร เช่น พายุ น้ำท่วม แผ่นดินไหว เป็นต้น อาจจะนำมาซึ่งความสูญเสียอย่างใหญ่หลวงกับระบบเทคโนโลยีสารสนเทศและการสื่อสารทำให้หยุดชะงัก ไม่สามารถให้บริการได้

๓.๗ เกิดจากจดหมายขยะ (Spam Mail)

มีโอกาสเกิดความเสี่ยงจากการได้รับจดหมายขยะเป็นจำนวนมาก อาจทำให้พื้นที่เก็บอีเมล์ในระบบคอมพิวเตอร์เต็ม และบางครั้งจดหมายขยะอาจมีไวรัสคอมพิวเตอร์ โทรจัน หรือหนอนคอมพิวเตอร์ ที่ทำให้เกิดความเสียหายต่อระบบคอมพิวเตอร์และเครือข่าย ทำให้เกิดการหยุดชะงัก ใช้งานไม่ได้ หรือขโมยข้อมูลสำคัญขององค์กรไป

๔. การเตรียมการเบื้องต้น

๔.๑ การให้ความรู้ความเข้าใจในการปฏิบัติงาน

เพื่อให้เจ้าหน้าที่และบุคลากรของหน่วยงานได้มีความรู้ความเข้าใจในการใช้งานระบบสารสนเทศได้อย่างถูกต้อง จึงได้มีการจัดทำคู่มือการใช้งานเพื่อเป็นแนวทางในการใช้งานและแก้ไขปัญหาเบื้องต้นได้อย่างมีประสิทธิภาพ และมีการจัดให้เจ้าหน้าที่บริหารจัดการระบบได้เข้าร่วมอบรม สัมมนาที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเพื่อเพิ่มพูนความรู้ความสามารถในการ บริหารจัดการระบบเทคโนโลยีสารสนเทศ และเผยแพร่ข้อมูลผ่านทางเว็บไซต์ http://it-sec.moj.go.th

๔.๒ การสำรองข้อมูล (Back up)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลถูกทำลายโดยไวรัสคอมพิวเตอร์ มีผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล เป็นต้น โดยสามารถนำข้อมูลที่จัดเก็บไว้กลับมาใช้งานทดแทนได้ทั้งแบบ Onsite และ Offsite

๔.๓ การป้องกันไวรัสหรือการเจาะระบบ

มีการติดตั้งระบบป้องกันการบุกรุก (Firewall) เพื่อปิดช่องโหว่ที่เสี่ยงต่อการที่ผู้ไม่ประสงค์ดีใช้ในการบุกรุกระบบ และติดตั้งโปรแกรมป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายเพื่อป้องกันผู้ไม่ประสงค์ดีใช้ในการบุกรุก หรือทำลายระบบ ทั้งนี้ผู้ใช้งานก็จำเป็นต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะในการเชื่อมต่อกับอินเทอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่ประสงค์ดีเข้ามาบุกรุก หรือทำลายระบบได้ โดยมีวิธีการดังนี้

๑) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลป้องกันไวรัสอยู่เสมอ
   - ติดตั้งโปรแกรมป้องกันไวรัส
   - อัพเดตข้อมูลป้องกันไวรัส
   - ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ
   - ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ ๑ ครั้ง

๒) ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ เช่น แผ่นซีดี แฮนดีไดรซ์ เป็นต้น
   - สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
   - ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่ไม่รู้จัก หรือน่าสงสัย เช่น .pif เป็นต้น
   - ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๓) ใช้ความระมัดระวังในการเปิดอีเมล์ (e-Mail)
   - อย่าเปิดไฟล์อีเมล์ที่ไม่ทราบแหล่งที่มา
   - ลบอีเมล์ทิ้งทันทีหากไม่ทราบแหล่งที่มา

๔) ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จากอินเทอร์เน็ต
   - ไม่ควรเปิดไฟล์ที่ไม่รู้จักที่แนบมากับโปรแกรมสนทนาต่างๆ เช่น Facebook ,Line
   - ไม่ควรเข้าไปเปิดเว็บไซต์ที่แนะนำมาทางอีเมล์ที่ไม่ทราบแหล่งที่มา
   - ไม่ดาวน์โหลดไฟล์จากเว็บไซต์ที่ไม่น่าเชื่อถือ
   - หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๕) ติดตั้ง Firewall เพื่อทำหน้าที่กำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก

๔.๔ การป้องกันจดหมายขยะ (Spam Mail)

ติดตั้งระบบป้องกันจดหมายขยะ (Mail Gateway) เพื่อคัดกรองและป้องกันการส่งจดหมายขยะขนาดใหญ่ หรือที่เรียกว่า Mail Bomb และมีมาตรการดังนี้

- กำหนดค่าสูงสุดของเนื้อที่เก็บอีเมล์ของแต่ละบัญชี
- มีการกำหนดจำนวนมากที่สุดที่ผู้ใช้แต่ละคนจะส่งได้ในแต่ละครั้ง
- กำหนดขนาดไฟล์ใหญ่ที่สุดของอีเมล์ที่จะรับได้
- ไม่อนุญาตให้ผู้ใช้ที่ไม่มีบัญชีบนระบบอีเมล์ส่งอีเมล์ผ่านไปยังที่อื่นได้
- มีการตรวจสอบว่าผู้ส่งอีเมล์มีอยู่จริง
- กำหนดนโยบายในการปฏิเสธการรับจดหมายจากการกำหนดคำใน Subject หรือ Domain Name หรือจาก IP Address

๔.๕ การป้องกันปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าขัดข้อง ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ

๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ทั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ที่สามารถสำรองไฟฟ้าได้นานประมาณ ๒๐-๓๐ นาที

๒) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๓) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

๔) สำหรับระบบไฟฟ้าสำรองในห้องคอมพิวเตอร์แม่ข่ายต้องมีการติดตั้งระบบแจ้งเตือนกระแสไฟฟ้าดับหรือไฟฟ้ากระชาก ซึ่งสามารถแจ้งเตือนเข้าสู่ระบบโทรศัพท์เคลื่อนที่ของเจ้าหน้าที่ผู้รับผิดชอบ และมีการบำรุงรักษาให้ระบบอยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๔.๖ การป้องกันไฟไหม้

เป็นการป้องกันการเกิดเพลิงไหม้ที่อาจจะเกิดกับห้องคอมพิวเตอร์แม่ข่าย ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ ดังนี้

๑) ติดตั้งระบบตรวจจับควันไฟความเร็วสูง เพื่อตรวจสอบการเกิดกลุ่มควันให้สามารถแจ้งเตือนด้วยเสียงกระดิ่ง และส่งข้อความเข้าสู่ระบบโทรศัพท์เคลื่อนที่ของเจ้าหน้าที่ผู้รับผิดชอบ ซึ่งทำให้สามารถควบคุมสถานะการณ์ได้ทันเวลา

๒) ติดตั้งระบบดับเพลิงอัตโนมัติ เพื่อตรวจจับความร้อนที่อาจจะก่อเป็นเพลิงไฟให้สามารถแจ้งเตือนและควบคุมเพลิงให้ดับลงโดยกระทบต่อระบบคอมพิวเตอร์และเครือข่ายน้อยที่สุด

๓) มีการทดสอบการใช้งานอย่างสม่ำเสมอเพื่อให้ระบบพร้อมใช้งานอยู่เสมอ

๔.๗ การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย โดยได้มีมาตรการดังนี้

๔.๖.๑ การป้องกันการบุกรุก การโจรกรรม และภัยคุกคามทางคอมพิวเตอร์ทางกายภาพ

๑) ให้มีการลงชื่อบันทึกข้อมูลเข้า-ออก เพื่อเป็นข้อมูลประวัติการเข้า - ออก

๒) ใช้ประตูปิดล็อคอัตโนมัติ เจ้าหน้าที่ผู้รับผิดชอบหรือได้รับมอบหมายเป็นผู้เปิดประตูให้เข้าเท่านั้น เพื่อป้องกันผู้ไม่ได้รับอนุญาตเข้าห้องคอมพิวเตอร์แม่ข่าย

๓) มีทีวีวงจรปิดบันทึกภาพการปฏิบัติงานตลอด ๒๔ ชั่วโมง เพื่อบันทึกการปฏิบัติงานในห้องคอมพิวเตอร์แม่ข่ายให้สามารถเรียกดูพฤติกรรมย้อนหลังที่น่าสงสัยได้

๔) จัดทำบัญชีคุมการใช้บัตรผ่านประตู (Key Card) ห้องศูนย์คอมพิวเตอร์ และปฏิบัติตามนโยบายความมั่นคงฯ และระเบียบปฏิบัติที่เกี่ยวข้อง

๔.๖.๒ การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ทางด้านเทคนิค

๑) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ไม่ได้รับอนุญาตจากระบบเครือข่ายเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๒) การเรียกใช้ระบบงาน (Application) ต่างๆ ผู้ใช้ระบบจะต้องผ่านระบบการตรวจสอบสิทธิ์การใช้งานก่อนการอนุญาตให้ใช้งานได้ตามอำนาจหน้าที่และความรับผิดชอบ

๓) การเรียกใช้งานบนระบบเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องทำการยืนยันตัวตนด้วยระบบการตรวจสอบสิทธิ์ ที่สามารถระบุตัวบุคคลทำให้ผู้ใช้มีความระมัดระวังมากขึ้นในการกระทำการต่างๆ บนระบบเครือข่ายอินเทอร์เน็ต

๔) ปฏิบัติตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ ของสำนักงานปลัดกระทรวงยุติธรรม และระเบียบที่เกี่ยวข้องที่สำนักงานปลัดกระทรวงยุติธรรมได้ประกาศใช้

๔.๘ การป้องกันการเกิดอุบัติภัยทางธรรมชาติหรือภัยคุกคามต่ออาคารที่ตั้งหน่วยงาน

เนื่องจากที่ตั้งหน่วยงานเป็นการเช่าสถานที่ อาคาร การบริหารจัดการสภาพแวดล้อมที่เกี่ยวข้องจึงเป็นหน้าที่ของอาคารในการบริหารจัดการเพื่อความมั่นคงปลอดภัยตามมาตรฐานของอาคาร ดังนั้นการป้องกันความเสียหายที่อาจเกิดจากอุบัติภัยทางธรรมชาติ เช่น พายุ น้ำท่วม แผ่นดินไหว หรืออาคารที่ตั้งหน่วยงาน เช่น การเกิดจลาจล หรือการปิดล้อมอาคาร จึงต้องปฏิบัติตามมาตรการที่ผู้รับผิดชอบอาคารกำหนด ทั้งนี้จะมีแผนในการจัดทำ DR Site (Disaster Recovery Site) ในอนาคตเพื่อเป็นศูนย์คอมพิวเตอร์ที่ให้บริการสำรองเมื่อศูนย์ให้บริการหลักไม่สามารถให้บริการได้

๔.๙ การจัดเตรียมอุปกรณ์ที่จำเป็น

ในการเตรียมความพร้อมรับภัยพิบัติที่อาจจะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารที่ทำให้ระบบคอมพิวเตอร์เกิดขัดข้อง ได้มีการจัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็น ดังนี้

๑) ระบบปฏิบัติการ (Operation System) และโปรแกรมสำคัญ ๆ ที่จำเป็น

๒) ระบบ Backup & Recovery

๓) ระบบสำรองไฟฟ้า (UPS)

๔) ระบบตรวจจับและดับเพลิง

๕) อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เช่น Hard disk, RAM, สาย LAN เป็นต้น

๖) โปรแกรม Anti Virus

๗) แผ่น Driver อุปกรณ์ต่างๆ

๘) เครื่องมือช่าง เช่น ไขควง, คีม, มีด, อุปกรณ์เข้าสาย LAN, ไฟฉาย เป็นต้น

๕. แนวทางปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

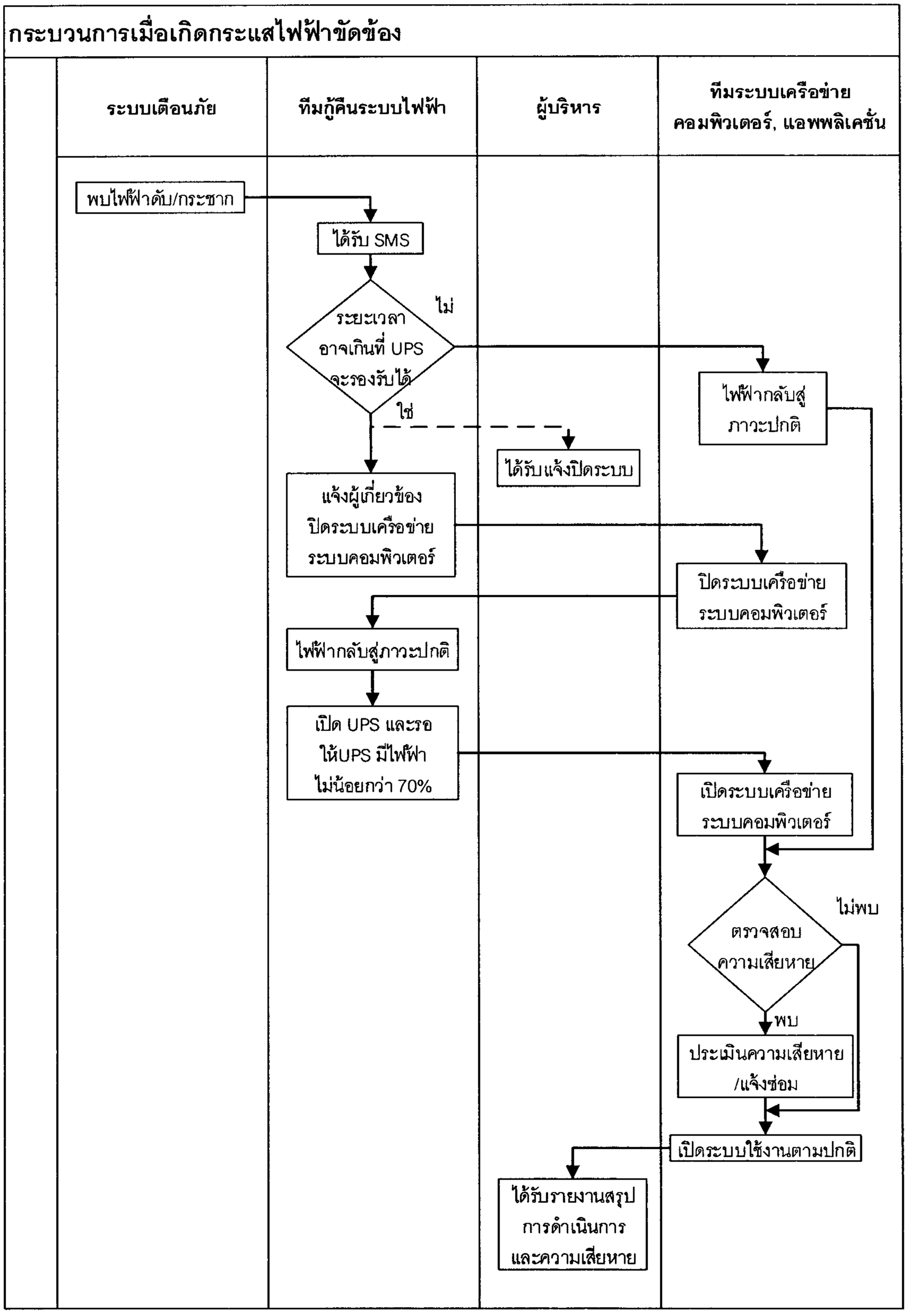
เมื่อเกิดภัยพิบัติขึ้นการดำเนินการจะแตกต่างกันไปตามแต่กรณี แต่จะมีแนวปฏิบัติเบื้องต้น ดังนี้

๑) ผู้พบเห็นเหตุการณ์ หรือผู้ควบคุมระบบทำการตรวจสอบสถานะการณ์เบื้องต้นว่าสามารถแก้ไขเหตุการณ์ได้หรือไม่

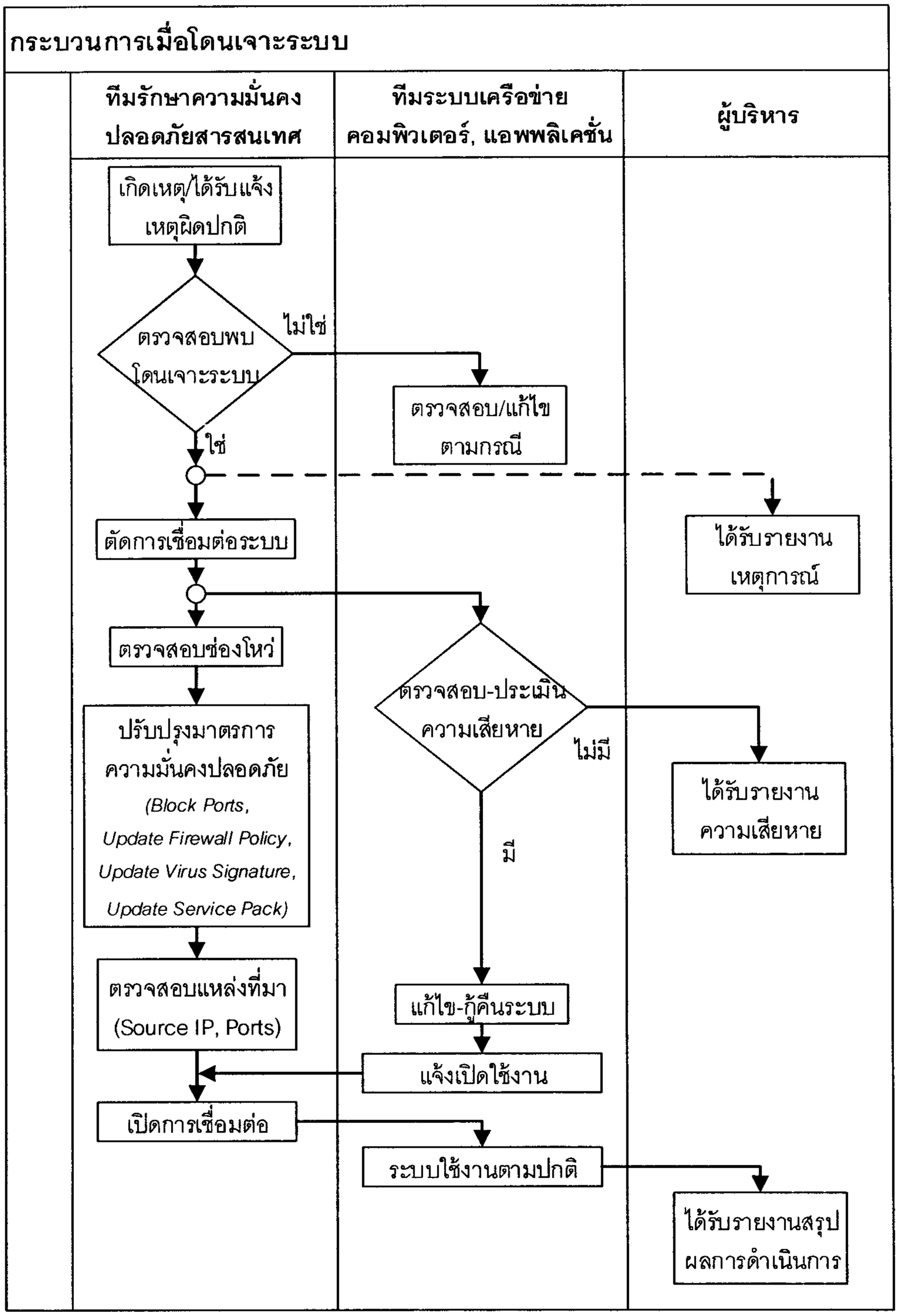
๒) หากไม่สามารถแก้ไขได้ ให้แจ้งผู้รับผิดชอบหรือผู้ที่เกี่ยวข้องเข้ามาดำเนินการแก้ไข

๓) ในกรณีที่เหตุการณ์รุนแรง อาจต้องอพยพคนไปยังสถานที่ปลอดภัยตามแผนปฏิบัติการที่เกี่ยวข้อง

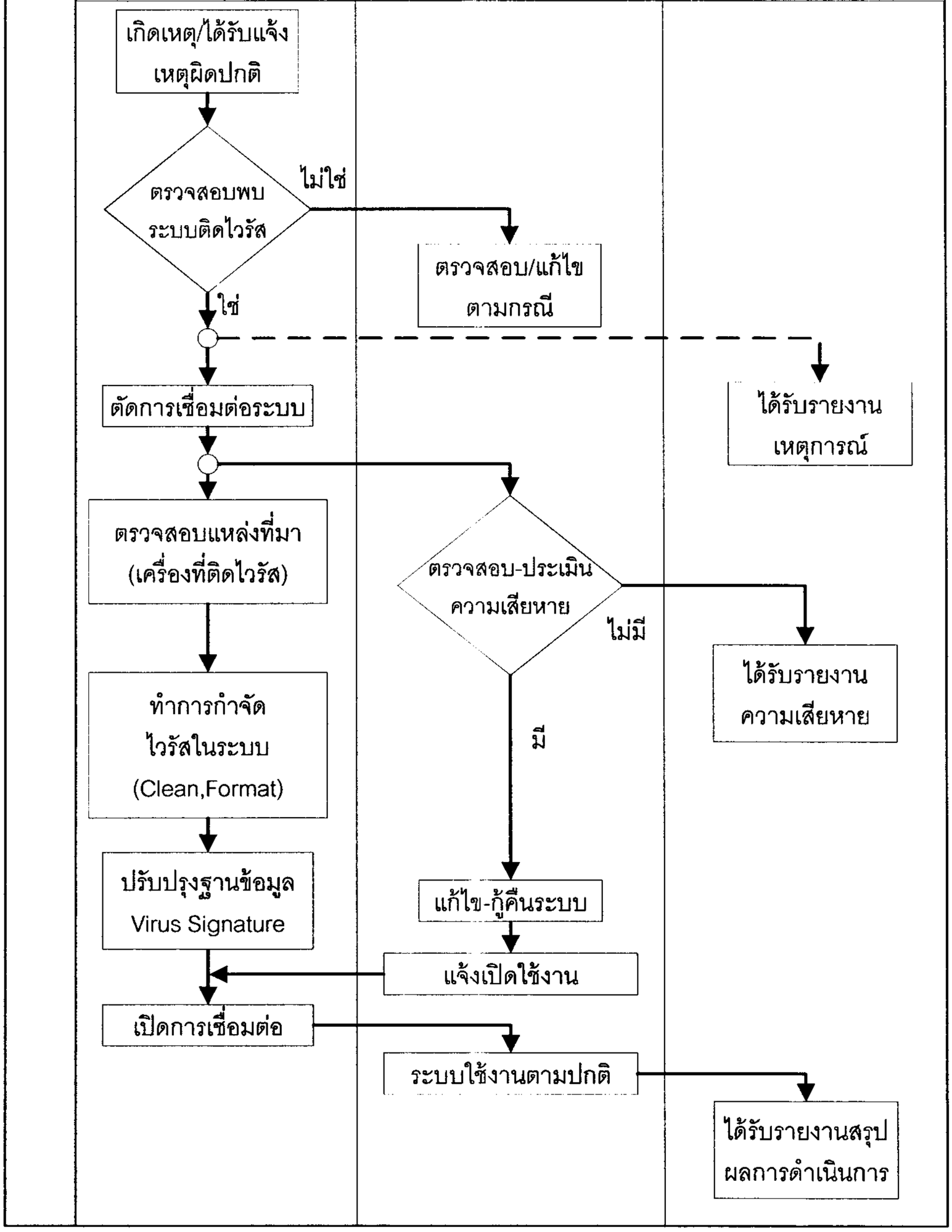
๕.๑ แนวปฏิบัติเมื่อเกิดภัยพิบัติจากกระแสไฟฟ้าขัดข้อง



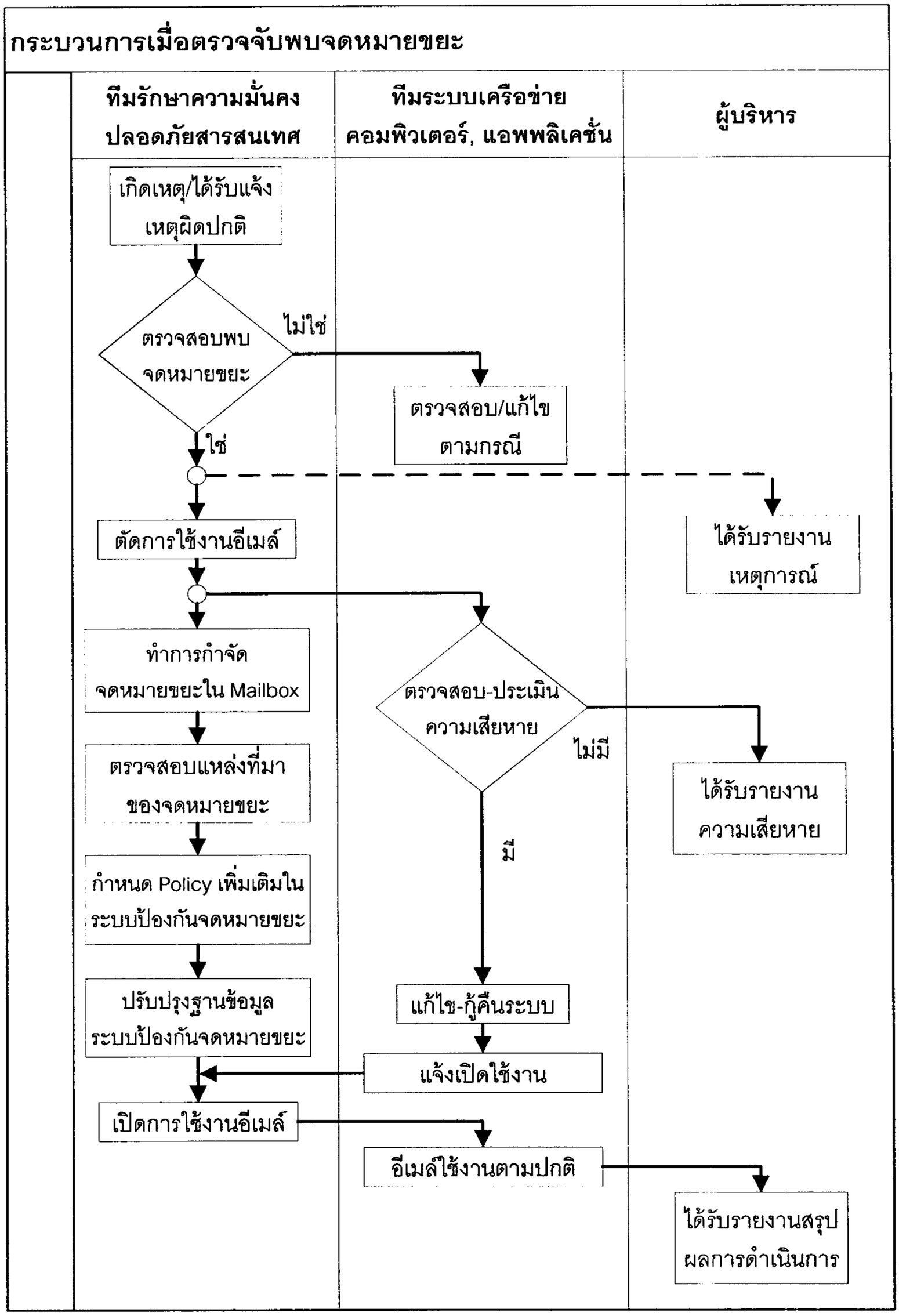
๕.๒ แนวปฏิบัติเมื่อเกิดเหตุขัดข้องจากการโดนเจาะระบบ



๕.๓ แนวปฏิบัติเมื่อระบบติดไวรัส

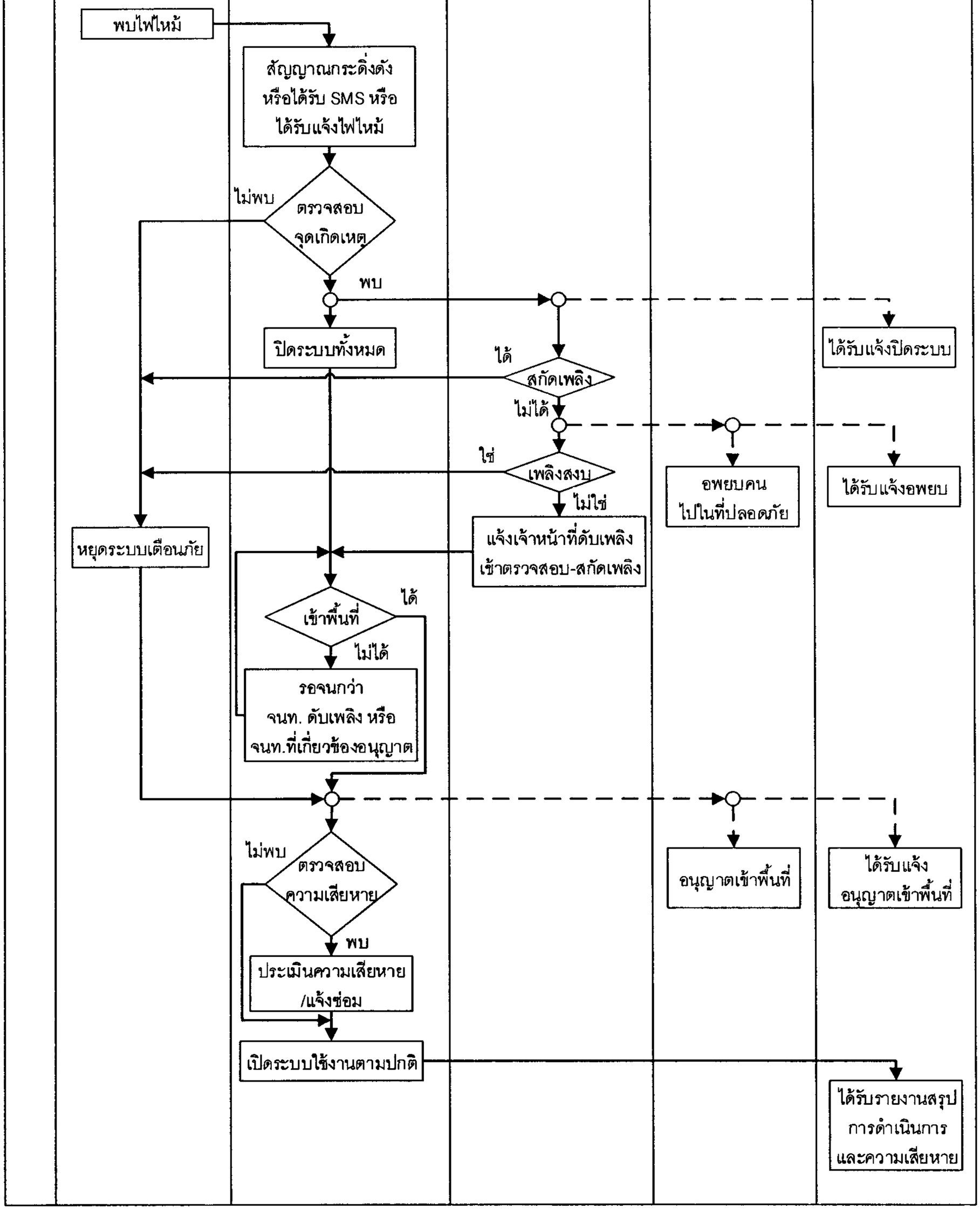


๕.๔ แนวปฏิบัติเมื่อตรวจจับพบจดหมายขยะ



๕.๕ แนวปฏิบัติเมื่อเกิดเหตุเพลิงไหม้

กระบวนการเมื่อเกิดเหตุเพลิงไหม้

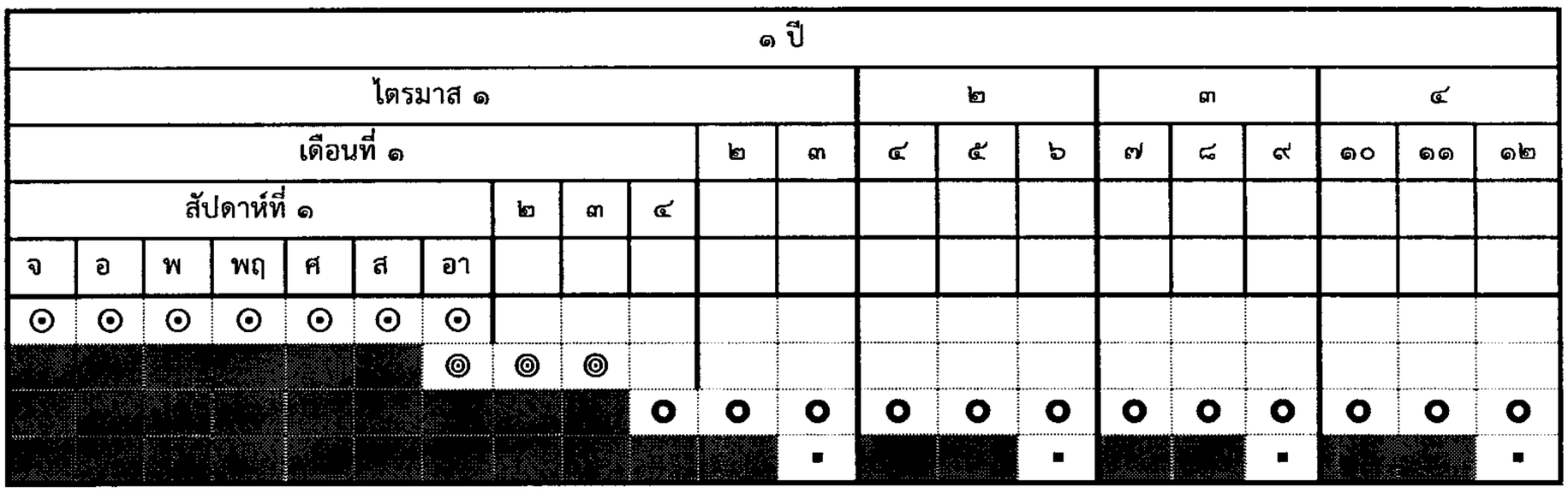


๖. การทำให้ระบบคอมพิวเตอร์และเครือข่ายกลับสู่สภาพปกติ

การกู้คืนระบบเครื่องแม่ข่าย (System Recovery) ซึ่งโดยปกติระบบเครื่องแม่ข่ายจะต้องอยู่ในสภาพพร้อมรองรับการให้บริการได้ตลอด ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้ก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้ เพื่อให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิมดังนี้

๖.๑ แนวทางในการสำรองข้อมูล

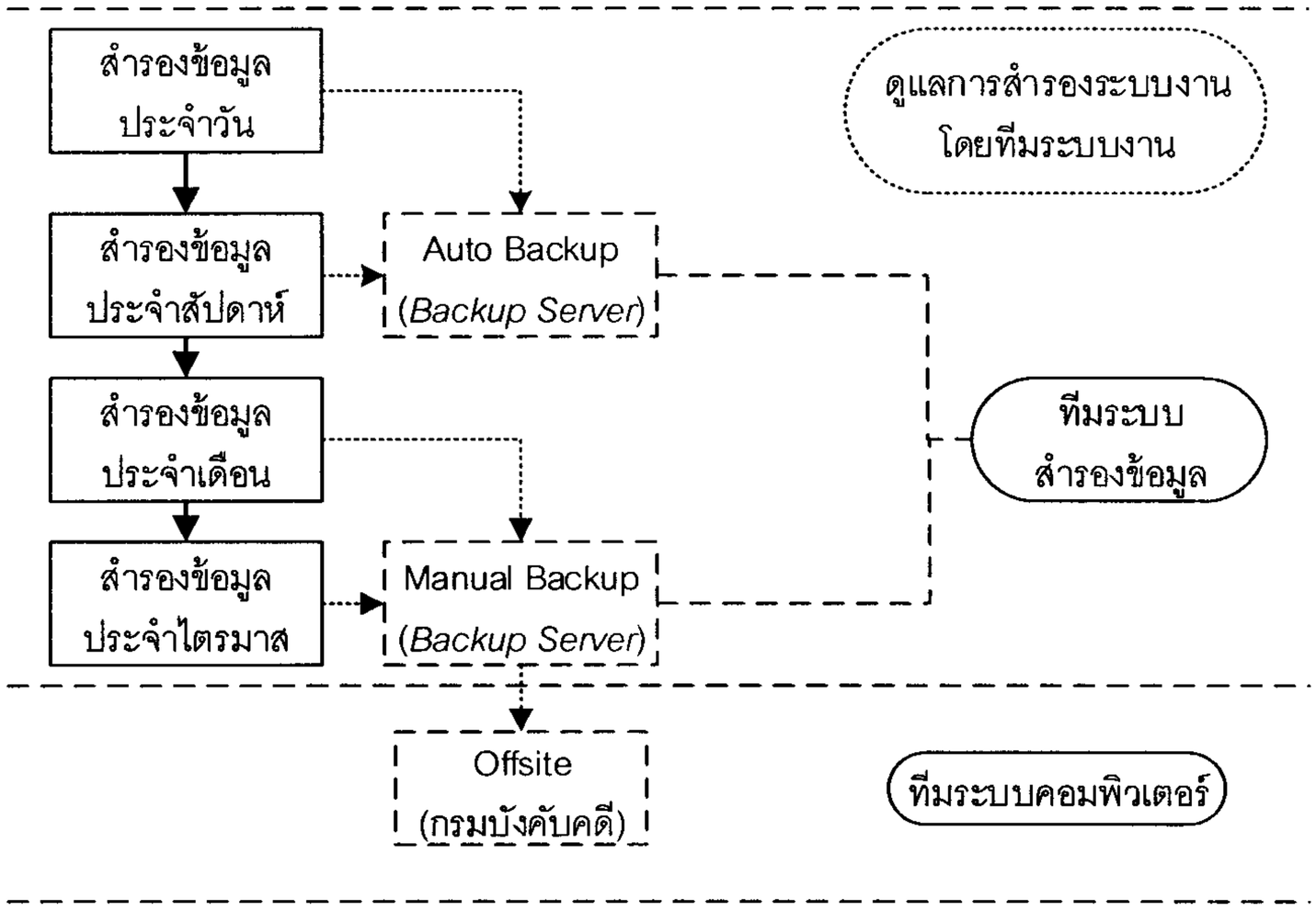
	ความถี่ในการสำรอง	รูปแบบข้อมูล	สื่อในการจัดเก็บ	จำนวน	ระยะเวลาที่เก็บ
๑	**ประจำวัน** ⊙ ทุกวัน (เวลา ๑๗.๐๐ น.)	Incremental / Differential - Configuration Backup Files - Application Files - Data Files	Auto-Backup (Int. HDD.)	๗ เวอร์ชั่น (ทุกวัน)	๑ สัปดาห์
๒	**ประจำสัปดาห์** ◎ ทุกวันเสาร์		Auto-Backup (Int. HDD.)	๔ เวอร์ชั่น (เดือนละ ๔ ครั้ง)	๑ เดือน
๓	**ประจำเดือน** ⭘ ทุกวันเสาร์สุดท้ายของเดือน		Manual-Backup (Ext. HDD.)	๒ เวอร์ชั่น (เดือนก่อน/ล่าสุด)	๒ เดือน
				สำเนา ๒ ชุด (Onsite/Offsite)	๑ ปี
๔	**ประจำไตรมาส (รอบ ๓ เดือน)** ■ ทุกวันเสาร์สุดท้ายของเดือนธันวาคม, มีนาคม, มิถุนายน, กันยายน	Full Backup (System + Data)	- Manual-Backup (Ext. HDD.)	๒ เวอร์ชั่น (ไตรมาสก่อน/ล่าสุด)	๖ เดือน
				๒ ชุด (Onsite/Offsite)	๑ ปี



⊙ ประจำวัน ◎ ประจำสัปดาห์

⭘ ประจำเดือน ■ ประจำไตรมาส

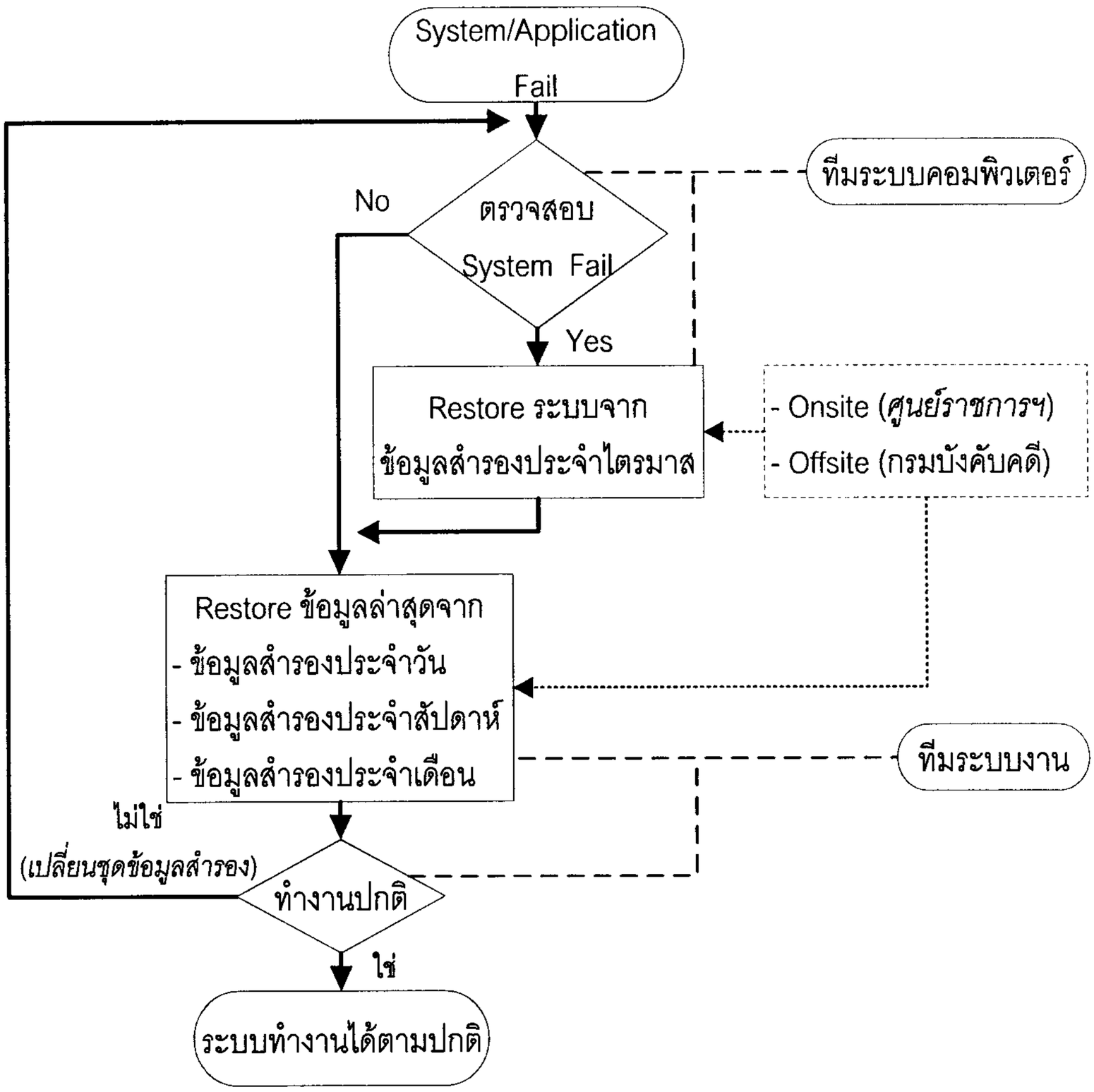
๖.๒ ขั้นตอนการสำรองข้อมูล



๖.๓ การติดป้าย (Label) บอกรายละเอียดการสำรองข้อมูลบนสื่อสำรองข้อมูล (DVD/Tape/External Hard disk)

Backup Description	
Server :	*[Server Name]*
Data Description :	*[Application / Database Name]*
Backup Type :	*[Data File | Full]*
Date :	*[DD / MM / YYYY]*
Media Number :	*[Number / Total]*

๖.๔ ขั้นตอนการกู้คืนระบบ



๗. ผู้รับผิดชอบและเบอร์โทรศัพท์ที่ติดต่อได้

หน้าที่ความรับผิดชอบของผู้เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ดังนี้

ผู้รับผิดชอบ	เบอร์โทรศัพท์
๗.๑ ระดับนโยบาย ได้แก่ ๑) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO ประจำกระทรวงยุติธรรม) ๒) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงยุติธรรม รับผิดชอบ กำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับดูแล ควบคุม ตรวจสอบการปฏิบัติงานของทีมปฏิบัติการ	๐๒ ๑๔๑ ๕๑๐๖ ๐๘๖ ๓๖๖ ๑๔๖๒ ๐๒ ๑๔๑ ๕๔๕๘ ๐๘๑ ๗๕๑ ๙๙๒๐
๗.๒ ระดับอำนวยการ ได้แก่ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงยุติธรรม รับผิดชอบ ๑) เป็นผู้บังคับบัญชาสูงสุดในการควบคุมการปฏิบัติการกรณีเกิดเหตุภัยพิบัติ ๒) มีอำนาจสั่งการให้ทุกหน่วยงานปฏิบัติการ หรือหยุดปฏิบัติการระงับเหตุภัยพิบัติ ๓) ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม ๔) รายงานข้อมูลสรุปผลการปฏิบัติการให้ CIO ประจำกระทรวงฯ ทราบ	๐๒ ๑๔๑ ๕๔๕๘ ๐๘๑ ๗๕๑ ๙๙๒๐
๗.๓ ระดับควบคุมและประสานงานกรณีเกิดเหตุภัยพิบัติ ได้แก่ ๑) ผู้อำนวยการส่วนยุทธศาสตร์และแผนเทคโนโลยีสารสนเทศ ๒) ผู้อำนวยการส่วนเทคโนโลยีระบบคอมพิวเตอร์และเครือข่าย ๓) ผู้อำนวยการส่วนพัฒนาระบบสารสนเทศและการจัดการเพื่อการบริหาร รับผิดชอบ ๑) วิเคราะห์สถานการณ์ในที่เกิดเหตุ และรายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ๒) สั่งการให้เจ้าหน้าที่ที่เกี่ยวข้องปฏิบัติตามแผน ๓) ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผนตามความเหมาะสมใน	๐๒ ๑๔๑ ๕๔๖๒ ๐๘๙ ๙๖๗ ๔๘๖๒ ๐๒ ๑๔๑ ๕๔๖๘ ๐๘๑ ๑๗๐ ๓๘๑๐ ๐๒ ๑๔๑ ๕๔๖๕ ๐๘๕ ๔๘๕ ๑๔๘๐

ผู้รับผิดชอบ	เบอร์โทรศัพท์
กรณีที่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารมอบหมายหรือไม่สามารถสั่งการได้ ๔) กำกับ ดูแล ให้คำปรึกษาในการปฏิบัติงานของทีมปฏิบัติการ	
๗.๔ ทีมปฏิบัติการกู้คืนระบบไฟฟ้า ได้แก่ ๑) นางสาวชัชนันท์ จันทบุรี นักวิชาการคอมพิวเตอร์ชำนาญการ ๒) นายสุรพงษ์ สุวรรณ์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ <u>รับผิดชอบ</u> เฝ้าระวัง ตรวจสอบ แก้ไขข้อบกพร่อง และจัดทำรายงานสรุปผลการปฏิบัติการกู้คืนระบบไฟฟ้า ในกรณีที่เกิดเหตุภัยพิบัติ	๐๒ ๑๔๑ ๕๔๗๓ ๐๘๙ ๔๖๑ ๔๕๐๐ ๐๒ ๑๔๑ ๕๔๗๒ ๐๘๗ ๕๖๖ ๑๔๘๐
๗.๕ ทีมปฏิบัติการกู้คืนระบบเครือข่ายและคอมพิวเตอร์ ได้แก่ ๑) นางสาวณัฏฐิณี แสงกุศลส่ง นักวิชาการคอมพิวเตอร์ชำนาญการ ๒) นายณัฐ นันติ นักวิชาการคอมพิวเตอร์ปฏิบัติการ <u>รับผิดชอบ</u> เฝ้าระวัง ตรวจสอบ แก้ไขข้อบกพร่อง และจัดทำรายงานสรุปผลการปฏิบัติการกู้คืนระบบเครือข่ายและคอมพิวเตอร์ ในกรณีที่เกิดเหตุภัยพิบัติ	๐๒ ๑๔๑ ๕๔๗๔ ๐๘๑ ๗๒๓ ๓๔๗๙ ๐๒ ๑๔๑ ๕๔๗๓ ๐๘๙ ๘๕๑ ๕๔๑๗
๗.๖ ทีมปฏิบัติการกู้คืนระบบแอพพลิเคชั่น ได้แก่ ๑) นายราเชน บุณยรัตพันธุ์ นักวิชาการคอมพิวเตอร์ชำนาญการ ๒) นายวีระพงศ์ ปริปัญญาปราชญ์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ ๓) นายธีระพล สันติสำราญวิไล นักวิชาการคอมพิวเตอร์ปฏิบัติการ <u>รับผิดชอบ</u> เฝ้าระวัง ตรวจสอบ แก้ไขข้อบกพร่อง และจัดทำรายงานสรุปผลการปฏิบัติการกู้คืนระบบแอพพลิเคชั่น ในกรณีที่เกิดเหตุภัยพิบัติ	๐๒ ๑๔๑ ๔๙๘๘ ๐๘๓ ๘๐๖ ๐๘๓๙ ๐๒ ๑๔๑ ๕๔๖๗ ๐๘๘ ๙๑๔ ๕๐๔๔ ๐๒ ๑๔๑ ๕๐๗๕ ๐๘๖ ๖๗๖ ๘๓๓๖

ผู้รับผิดชอบ	เบอร์โทรศัพท์
๗.๗ ทีมปฏิบัติการควบคุมเพลิงขั้นต้น ได้แก่ ๑) นายคเณศศักดิ์ ชัยอินทร์ นักวิชาการคอมพิวเตอร์ชำนาญการ ๒) นายสุรพงษ์ สุวรรณ์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ <u>รับผิดชอบ</u> เฝ้าระวัง ตรวจสอบ แก้ไขข้อบกพร่อง และจัดทำรายงานสรุปผลการปฏิบัติการควบคุมเพลิงขั้นต้น ในกรณีที่เกิดเหตุภัยพิบัติ	๐๒ ๑๔๑ ๕๔๗๓ ๐๘๕ ๘๓๘ ๘๑๐๐ ๐๒ ๑๔๑ ๕๔๗๒ ๐๘๗ ๕๖๖ ๑๔๘๐
๗.๘ ทีมปฏิบัติการอพยพคน ได้แก่ ๑) นายคเณศศักดิ์ ชัยอินทร์ นักวิชาการคอมพิวเตอร์ชำนาญการ ๒) นางสาวสุปราณี ลาภโภคาชัย นักวิชาการคอมพิวเตอร์ปฏิบัติการ ๓) นางสาวรุ่งนภา ศิริลักษณะพงศ์ นักจัดการงานทั่วไปปฏิบัติการ ๔) นายภาคิน ตัณฑ์ณรงค์ เจ้าหน้าที่เครื่องคอมพิวเตอร์ <u>รับผิดชอบ</u> เฝ้าระวัง ตรวจสอบ ประสานงาน ประชาสัมพันธ์ในการปฏิบัติการอพยพคนในกรณีที่เกิดเหตุภัยพิบัติ	๐๒ ๑๔๑ ๕๔๗๓ ๐๘๕ ๘๓๘ ๘๑๐๐ ๐๒ ๑๔๑ ๕๔๖๗ ๐๘๑ ๘๘๐ ๕๓๕๑ ๐๒ ๑๔๑ ๕๔๖๐ ๐๘๐ ๓๒๖ ๑๔๓๖ ๐๒ ๑๔๑ ๕๔๗๒ ๐๙๙ ๒๕๗ ๔๖๕๖
๗.๙ ทีมปฏิบัติการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ได้แก่ ๑) นางสาวณัฏฐิณี แสงกุศลส่ง นักวิชาการคอมพิวเตอร์ชำนาญการ ๒) นายณัฐ นันติ นักวิชาการคอมพิวเตอร์ปฏิบัติการ <u>รับผิดชอบ</u> เฝ้าระวัง ตรวจสอบ แก้ไขข้อบกพร่อง และจัดทำรายงานสรุปผลการปฏิบัติการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ในกรณีที่เกิดเหตุภัยพิบัติ	๐๒ ๑๔๑ ๕๔๗๔ ๐๘๑ ๗๒๓ ๓๔๗๙ ๐๒ ๑๔๑ ๕๔๗๓ ๐๘๙ ๘๕๑ ๕๔๑๗
๗.๑๐ ทีมปฏิบัติการดูแลระบบคอมพิวเตอร์และเครือข่ายประจำวัน ได้แก่ ๑) นางสาวณัฏฐิณี แสงกุศลส่ง นักวิชาการคอมพิวเตอร์ชำนาญการ	๐๒ ๑๔๑ ๕๔๗๔ ๐๘๑ ๗๒๓ ๓๔๗๙

ผู้รับผิดชอบ		เบอร์โทรศัพท์
๒) นายคเณศศักดิ์ ชัยอินทร์	นักวิชาการคอมพิวเตอร์ชำนาญการ	๐๒ ๑๔๑ ๕๔๗๒ ๐๘๕ ๘๓๘ ๘๑๐๐
๓) นางสาวชัชนันท์ จันทบุรี	นักวิชาการคอมพิวเตอร์ชำนาญการ	๐๒ ๑๔๑ ๕๔๗๓ ๐๘๙ ๔๖๑ ๔๕๐๐
๔) นายณัฐ นันติ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒ ๑๔๑ ๕๔๗๓ ๐๘๙ ๘๕๑ ๕๔๑๗
๕) นายสุรพงษ์ สุวรรณ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒ ๑๔๑ ๕๔๗๒ ๐๘๗ ๕๖๖ ๑๔๘๐
๖) นางสาวเกศกนก อัศวโยธิน	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒ ๑๔๑ ๕๔๗๓ ๐๘๗ ๗๑๙ ๐๕๐๕
๗) นางสาวน้ำทิพย์ ฉิมสุด	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒ ๑๔๑ ๕๔๗๕ ๐๙๕ ๕๘๔ ๒๙๙๒
<u>รับผิดชอบ</u> เฝ้าระวัง ตรวจสอบ แก้ไขข้อบกพร่องเกี่ยวกับการทำงานของระบบคอมพิวเตอร์ แม่ข่ายและระบบเครือข่ายคอมพิวเตอร์ รวมไปถึงการเกิดเหตุภัยพิบัติในวันที่เข้าปฏิบัติการ		
๗.๑๑ ทีมปฏิบัติการระบบสำรองข้อมูล (Backup Server) ได้แก่		
๑) นายสุทธิโชค คนโซเงิน	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒ ๑๔๑ ๕๑๕๓ ๐๙๑ ๔๗๘ ๔๗๖๘
๒) นายสุรพงษ์ สุวรรณ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒ ๑๔๑ ๕๔๗๒ ๐๘๗ ๕๖๖ ๑๔๘๐
๓) นางสาวเกศกนก อัศวโยธิน	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๒ ๑๔๑ ๕๔๗๓ ๐๘๗ ๗๑๙ ๐๕๐๕
<u>รับผิดชอบ</u> ติดตั้ง ตรวจสอบ แก้ไขข้อบกพร่องเกี่ยวกับการทำงานของระบบสำรองข้อมูล		

ผู้อนุมัติแผนฯ

พันตำรวจเอก .....)

(ดุษฎี อารยวุฒิ)

รองปลัดกระทรวงยุติธรรม

ปฏิบัติราชการแทน ปลัดกระทรวงยุติธรรม

ภาคผนวก

กระบวนการในการแจ้งเตือนภัย